

REMARKS

Please make the amendments herein prior to examination.

Applicants respectfully request reconsideration.

Applicants' attorney wishes to thank Examiner Meislahn for the courtesies extended during the telephone interview of October 9, 2001. The Examiner's interview summary dated October 22, 2001 states that it is the Examiner's position that the term "by a multi-client manager" does not preclude a user from choosing the expiry data. Again, Applicants respectfully point out that the claims, for example, Claim 1 and others require providing, by a multi-client manager unit, selectable digital signature expiry data including at least public verification key expiry data and selectable private signing key expiry data that are selectable on a per client basis through the multi-client manager unit. As further noted in Applicants' previous responses, the multi-client manager unit as claimed is a type of trust authority and as such a user does not have access to change trust or expiry data information, otherwise such a system would become basically unprotected. Accordingly, Applicants respectfully submit that the claimed invention does preclude a user from choosing the expiry data. Applicants also respectfully reassert the relevant remarks made in previous Responses to Office Actions.

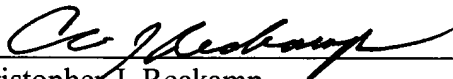
In addition, Applicants have amended dependent claims 5, 19 and 25 to note other distinguishing features, namely that the initiation of a digital signature key pair update request is based on multiple criteria including, for example, whether a difference between a current date and the digital signature private key lifetime end date is less than an absolute predetermined period of time and based on whether the difference between the current date and the digital signature private key lifetime end date is less than a selectable predetermined percentage of a total duration of a digital signature private key lifetime. (See also, for example, Specification, p. 7, ll. 27-31). Accordingly, the multi-client manager unit selectable predetermined percentage that is based on, for example, a period of time such as 50% or less or more of a total duration of an encryption private key lifetime or any suitable period of days or other time period. Such a system is not taught or suggested by the cited references. Accordingly, these claims are believed to be allowable.

As to Claim 3, the Lewis reference merely states that the key service sends a key replacement message to each node or broadcast a single key replacement message. There is no mention of a privilege control. The claimed method includes, inter alia, providing variable update privilege control on a per client basis to facilitate denial of updating the digital signature key pair on a per client basis. No denial control is taught or suggested by the cited references. As To Claim 6, Ellison is silent as to a multi-client manager unit having, among other things, a user interface that facilitates setting of selectable expiry data on a per client basis.

Applicants respectfully reassert the remarks made with respect to the other claims in previous responses to Office Actions. Accordingly, Applicants respectfully submit that the claims are in condition for allowance and an early Notice of Allowance is respectfully solicited.

Also, attached hereto is a marked-up version of the changes made to Claims 1 by the current amendment. The attached page is captioned: "Version with Markings to Show Changes Made."

Respectfully submitted,

By: 
Christopher J. Reckamp
Registration No. 34,414

Date: November 5, 2001

VEDDER, PRICE, KAUFMAN &
KAMMHOLZ
222 N. LaSalle Street
Chicago, IL 60601
(312) 609-7500; FAX: (312) 609-5005

VERSION WITH MARKINGS TO SHOW CHANGES MADE

5. (Once amended) The method of claim 1 further comprising the steps of:

determining a digital signature private key lifetime end date and a digital signature certificate creation date upon a user login to the public key system;

initiating, by a client unit, a digital signature key pair update request based on whether a difference between a current date and the digital signature private key lifetime end date (t1) is less than an absolute predetermined period of time [(days)] and based on whether the difference between the current date and the digital signature private key lifetime end date (t1) is less than a selectable predetermined percentage of a total duration of a digital signature private key lifetime.

19. (Once amended) The system of claim 14 further comprising:

means for determining a digital signature private key lifetime end date and a digital signature certificate creation date upon a user login to the public key system;

client means for initiating a digital signature key pair update request based on whether a difference between a current date and the digital signature private key lifetime end date (t1) is less than an absolute predetermined period of time [(days)] and based on whether the difference between the current date and the digital signature private key lifetime end date (t1) is less than a selectable predetermined percentage of a total duration of a digital signature private key lifetime.

25. The storage medium of claim 21 wherein the stored program further facilitates the steps of:

determining a digital signature private key lifetime end date and a digital signature certificate creation date upon a user login to the public key system;

initiating, by a client unit, a digital signature key pair update request based on whether a difference between a current date and the digital signature private key lifetime end date (t1) is less than an absolute predetermined period of time [(days)] and based on whether the difference between the current date and the digital signature private key lifetime end date (t1) is less than a selectable predetermined percentage of a total duration of a digital signature private key lifetime.